



UNITED STATES PATENT AND TRADEMARK OFFICE

MN
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/684,964	10/14/2003	Thomas Henry Ptacek	0016.0011	9948
29127	7590	04/06/2007		
HOUSTON ELISEEVA 4 MILITIA DRIVE, SUITE 4 LEXINGTON, MA 02421			EXAMINER BLUDAU, BRANDON S	
			ART UNIT 2132	PAPER NUMBER

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/684,964	PTACEK ET AL.	
	Examiner	Art Unit	
	Brandon S. Bludau	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 October 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-34 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-34 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) ☒ Notice of References Cited (PTO-892) | 4) ☐ Interview Summary (PTO-413) |
| 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) ☒ Information Disclosure Statement(s) (PTO/SB/08) | 5) ☐ Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) ☐ Other: _____ |

DETAILED ACTION

1. Claims 1-34 are examined.

Double Patenting

A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

2. Claims 1-34 are provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claims 1-34 of copending Application No. 10/887213. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 21 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 6 cites generating instructions, however, there is no clear function of the instructions.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-10,12-14,18,21-29 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Copeland (US PgPub 2002/0144156).

5. As per claim 1, Copeland discloses a system for controlling communications over a computer network, the system comprising:

access control devices for the computer network that control communications between compartments of the computer network [0059];

attack detection system for determining whether the computer network may be under attack [0062]; and

a control plane for instructing the access control devices to allow network communications between the compartments of the computer network based on a usage model describing legitimate network communications while restricting other network communications between the compartments, in response to attack [0066] and [0166].

The examiner notes that Copeland doesn't explicitly disclose multiple access control devices that control communications between compartments of the network, however, as shown in fig.2 the network is described in simple terms. It would have been obvious for one of ordinary skill in the art to view the inside network as containing more than 2 computers and necessarily more than one network device controlling

Art Unit: 2132

access to the multitude of computers, thus it would have been obvious that the plural network devices necessarily compartmentalize the network and each would maintain a separate port profiling engine as necessarily implied.

6. As per claim 2, Copeland discloses a system as claimed in claim 1, wherein the computer network is an enterprise network ([0057] wherein it would have been apparent that an organization may necessarily embody an enterprise network).

7. As per claim 3, Copeland discloses a system as claimed in claim 1, but does not explicitly disclose wherein the computer network is a service provider network. The Examiner argues that the method of network profiling could be used on any network concerned with monitoring communications, moreover, nothing in Copeland precludes the method from being embodied in a service provider network, thus this would have been an obvious modification over Copeland, as would have been readily apparent to one of ordinary skill in the art.

8. As per claim 4, Copeland discloses a system as claimed in claim 1, wherein the computer network is a public network. See arguments above, moreover, Fig. 1 discusses a public network using the Internet.

9. As per claim 5, Copeland discloses a system as claimed in claim 1, wherein the access control devices compartmentalize the computer network into separate sub-networks of network devices. The Examiner argues this obviousness and necessity above in the rejection to claim 1.

10. As per claim 6, Copeland discloses a system as claimed in claim 1, wherein the access control devices separate host computers from the computer network (see fig. 2).

11. As per claim 7, Copeland discloses a system as claimed in claim 1, further comprising a network modeling system for generating the usage model ([0062] and [0068]-[0076]).

12. As per claim 8, Copeland discloses a system as claimed in claim 7, wherein the network modeling system receives flow information describing communications between network devices [0059].

13. As per claim 9, Copeland discloses a system as claimed in claim 8, wherein the flow information is collected by network communications devices [0059].

14. As per claim 10, Copeland discloses a system as claimed in claim 8, wherein the flow information is collected by the access control devices ([0059] wherein the access control device is item 135 in figure 2).

15. As per claim 12, Copeland discloses a system as claimed in claim 7, wherein the network modeling system compares new network communications to the usage model and updates the usage model if the new network communications are not described by the usage model [0062] and [0069].

16. As per claim 13, Copeland discloses a system as claimed in claim 1, wherein entries in the usage model comprise source addresses, destination addresses, source ports, and destination ports derived from the network communications [0054]-[0056].

17. As per claim 14, Copeland discloses a system as claimed in claim 1, wherein entries in the usage model comprise source addresses, destination addresses, source ports, and destination ports derived from the network communications in addition to time stamp information indicating when the network communication was last detected [0055].

Art Unit: 2132

18. As per claim 18, Copeland discloses a system as claimed in claim 1, wherein the attack detection system monitors communications over the computer network for attack by monitoring changes in connections between network devices ([0055] wherein all connection changes are necessarily monitored).

19. Claim 21 is rejected because it discloses substantially similar subject matter to claim 1.

20. Claims 22 and 23 are rejected because they disclose substantially similar subject matter to claim 8.

21. Claim 24 is rejected because it discloses substantially similar subject matter to claim 13.

22. Claims 25 and 26 are rejected because they disclose substantially similar subject matter to claims 5 and 6 respectively.

23. Claim 27 is rejected because it discloses substantially similar subject matter to claim 8.

24. Claim 28 is rejected because it discloses substantially similar subject matter to claim 10.

25. Claim 29 is rejected because it discloses substantially similar subject matter to claim 12.

26. Claim 32 is rejected because it discloses substantially similar subject matter to claim 18.

27. Claims 11, 16-17, 19-20, 30-31 and 33-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Copeland (US 2002/0144156) and further in view of Yadav (US PgPub 2003/0149888).

28. As per claim 11, Copeland discloses a system as claimed in claim 8, but does not disclose wherein the network modeling system discards flow information between network devices in the computer network and network devices external to the computer network. The examiner argues that it would have been obvious for one of ordinary skill in the art to modify Copeland to include wherein only communications within the network were examined, moreover the Examiner admits Yadav for also disclosing this feature.

Yadav discloses a method of network intrusion detection wherein the access control component resides on a networked machine [0022] and fig. 2b, wherein the network may be a single network wherein communications from within the network are only monitored for attack/intrusion (as discussed in [0002] and [0005]). Yadav is analogous art because it is directed to a method of intrusion detection in a network. It would have been obvious to supplement Copeland to include wherein only flow information between internal network devices was monitored. Motivation for one of ordinary skill in the art to modify Copeland as discussed above would have been to implement the method wherein it is desirable to detect for intrusion attacks only within the network devices as may be desirable for certain single networks, as would have been obvious to one of ordinary skill in the art and as is implied as a choice embodiment in [0002] and [0005] of Yadav.

Art Unit: 2132

29. As per claim 16, Copeland discloses a system as claimed in claim 1, but does not explicitly disclose wherein the attack detection system monitors communications over the computer network for attack using signature detection.

Yadav discloses such a method of detecting intrusion based on signature analysis ([0032]). Yadav is analogous art because it is directed to a method of network intrusion detection. It would have been obvious to modify Copeland to include a method of detecting intrusion based on signature attacks. Motivation for modifying Copeland as discussed above would have been readily apparent to one of ordinary skill in the art, as it is a well-known and common method to scan for known intrusion behavior.

30. As per claim 17, Copeland discloses a system as claimed in claim 1, but does not explicitly disclose wherein the attack detection system performs heuristic modeling to determine whether the computer network is under attack. The examiner argues that heuristic modeling is a well-known method of detecting abnormal behavior moreover, Yadav disclose such heuristic methods (see claim 25). It would have been obvious in view of Yadav to disclose intrusion detection based on heuristic modeling as it was a well-known method at the time of the invention.

31. As per claim 19, Copeland discloses a system as claimed in claim 1, but does not explicitly disclose wherein the control plane receives protocol information and/or port information characteristic of the attack and generates pass and/or blocking rules for the access control devices. While Copeland doesn't explicitly disclose this feature, it would have been understood in view of the entire disclosure, moreover The Examiner admits Yadav as a supplement to disclose the common feature in the art.

Yadav disclose such a method wherein pass/blocking rules are generated for the access control devices ([0028]). Motivation for modifying Copeland to include generating pass/blocking rules base don protocol or port information would have been well known and understood by one of ordinary skill in view of Copeland, as it is a necessary feature.

32. As per claim 20, Copeland discloses a system as claimed in claim 1, but does not explicitly disclose wherein the control plane receives protocol information and/or port information characteristic of the attack and generates pass rules and blocking rules for the access control devices, in which the pass rules are generated from the usage model and the blocking rules are generated from the protocol information and/or port information characteristic of the attack [0028] and [0029] see arguments above in view of claim 19.

33. Claims 30 and 31 are rejected because they disclose substantially similar subject matter to claims 16 and 17 respectively.

34. Claims 33 and 34 are rejected because they disclose substantially similar subject matter to claims 18 and 20 respectively.

35. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Copeland (US 2002/0144156) and further in view of Day (US Patent 7017186).

36. As per claim 15, Copeland discloses a system as claimed in claim 1, wherein entries in the usage model comprise source addresses, destination addresses, source ports, and destination ports derived from the network communications ([0054]-[0056])but does not specifically disclose additionally storing frequency information

indicating a frequency of the network communication. The Examiner argues that the profiling references each communication thus frequency determination may be made based on the stored table.

Moreover, Day discloses a method of detecting network intrusion wherein frequency data of a specific field is stored in addition to address, port and protocol information (column 8 lines 26-50). Day is analogous art because it is directed to a method of network intrusion detection. It would have been obvious for one of ordinary skill in the art to modify Copeland to include storing frequency data relating to a particular communication instance. Motivation for modifying Copeland as discussed above would have been to enhance the profiling of network activity by calculating historical data for frequency of a communication, as it is well known to one of ordinary skill that a single communication may not raise alarm, however if a plurality of the same communication is evident beyond a certain threshold this may be an alarming event.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Jackson (US PgPub 2004/0103211), Sheymov (US PgPub 2002/0023227), Lee (US PgPub 2004/0015719), Shipley (US Patent 6119236).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Bludau whose telephone number is 571-272-3722. The examiner can normally be reached on Monday -Friday 8:00-5:30.

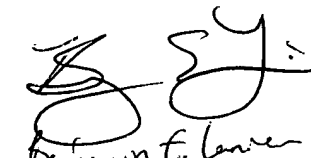
Art Unit: 2132

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BB

Brandon S Bludau
Examiner
Art Unit 2132


Benjamin E. Lawrence
Examiner Art Unit 2132